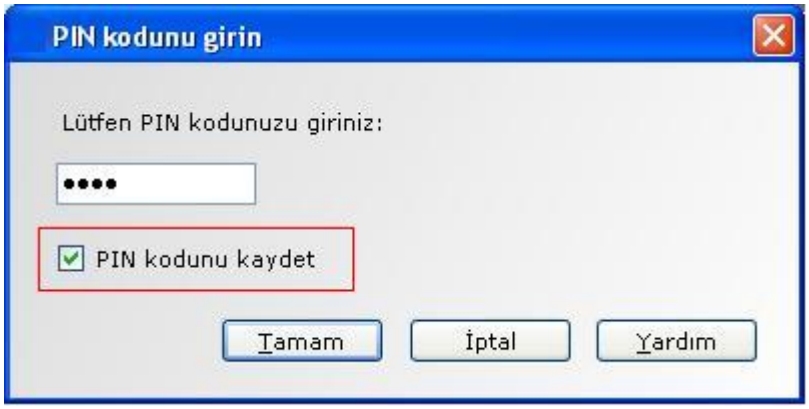
3G USB

written by Mert SARICA | 23 December 2009

Yine canımın sıkıldığı bir günde bir arkadaşım 3G USB modeminden bahsediyordu, birden ilgimi çekti, daha önce inceleme fırsatıda bulamamıştım. Kendisi bana kısa bir demo yaparak 3G USB modem ile gelen ve Huawei tarafından geliştirilen mobil uygulamanın (Not: Türkiye'deki GSM operatörleri tarafından 3G USB modem ile dağıtılan mobil uygulamaların geliştiricisi Huawei'dir) nasıl kullanıldığını kısaca gösterdi. İlk dikkatimi çeken bu programda Save Pin özelliğinin olmasıydı (kısaca Internet Explorer'ın remember me özelliği gibi düşünebilirsiniz.) çünkü bu özelliğin olması PIN'in, diskte bir yerlerde saklanması anlamına geliyordu.



Bunun dışında bu mobil uygulamanın 3G USB modem ile nasıl haberleştiği merakımı cezbetmişti, uygulama ile modem arasındaki haberleşmede PIN açık mı gidiyordu yoksa şifreli mi gidiyordu (şifreli olarak gitmesi ve smartcard üzerinde decrypt edilmesi teknik olarak mümkün mü bilmiyorum) bu konuda merak konusu olmuştu. Bunlar dışında 3G USB modem ile kısa mesaj almak ve göndermekte mümkün oluyordu. SMS alıp verme hadisesi hemen aklıma yakın zamanda Türkiye'deki tüm bankalarda hayata geçecek olan tek kullanımlık şifre uygulamasını getirdi.

Bilindiği üzere 1 Ocak 2010 tarihinden itibaren tüm bankalar için tek kullanımlık şifre uygulaması zorunlu hale geliyor. Bu yeni uygulama ile müşteriler, internet bankacılığına girmek için ilgili banka tarafından kendisine kısa mesaj aracılığıyla gönderilen tek kullanımlık şifreyi kullanacaklar. Bunun için müşterinin banka kayıtlarında güncel cep telefonu numarasının bulunması şart.

Peki ya güncel değilse ? Bu durumda müşteri cep telefonu numarasını

güncellemek için ilgili bankanın hizmet merkezini arayarak cep telefonu numarasını güncelleyecek. Buraya kadar herşey normal ancak aklıma şöyle bir soru takıldı. Ya geek bir müşteri hazırda 3G USB modemi varken ve mobil uygulama ile SMS alabiliyorken müşteri hizmetlerine cep telefonu numarası yerine 3G USB modeminde kullandığı numarasını verirse ne olacak ? Bu durumda hem internet bankacılığına girmek ve hem de finansal işlemler gerçekleştirebilmek için kullanacağı tek kullanımlık şifre bilgisayarına ulaşacak ve kolayca bu şifreye ulaşabilecek ve kullanabilecek. Peki ya güvenlik ?

İşte bu soruya yanıt ararken kendi kendime bir senaryo ürettim. Bir trojan düşündüm. Malum internet bankacılığında kritik işlemler öncesinde (örnek para transferi) tek kullanımlık şifreler ile müşteriler doğrulanıyor. Peki ya bu tek kullanımlık şifre 3G USB modeme geliyorsa ? Bu durumda trojan kullanıcının haberi olmadan internet tarayıcısına çengel atarak para transferi işlemi esnasında istenilen tek kullanımlık şifreyi 3G mobil uygulamasından alabilir ve kendi kendine finansal işlem gerçekleştirebilir miydi ? Muhtemelen evet…

Örnekleri ile daha öncede karşılaştığımız üzere artık yeni nesil malwareler internet tarayıcılarına çengel atarak GET/POST edilen verileri kayıt altına alıyorlar. 3G USB modemlerin yaygınlaşması ve insanların kullandıkları hatları tek kullanımlık şifre içinde kullanmaları durumunda artık art niyetli kişilerin işleri daha da kolaylaşacak gibi görünüyor…

Bu yazıyı yazmamdaki asıl amaç bu konuya dikkat çekmek ve insanların tek kullanımlık şifre için cep telefonlarını kullanmaya devam etmelerini önermekti ancak diğer bir yandan merak ettiğim konularada yanıt aramaya karar verdim.

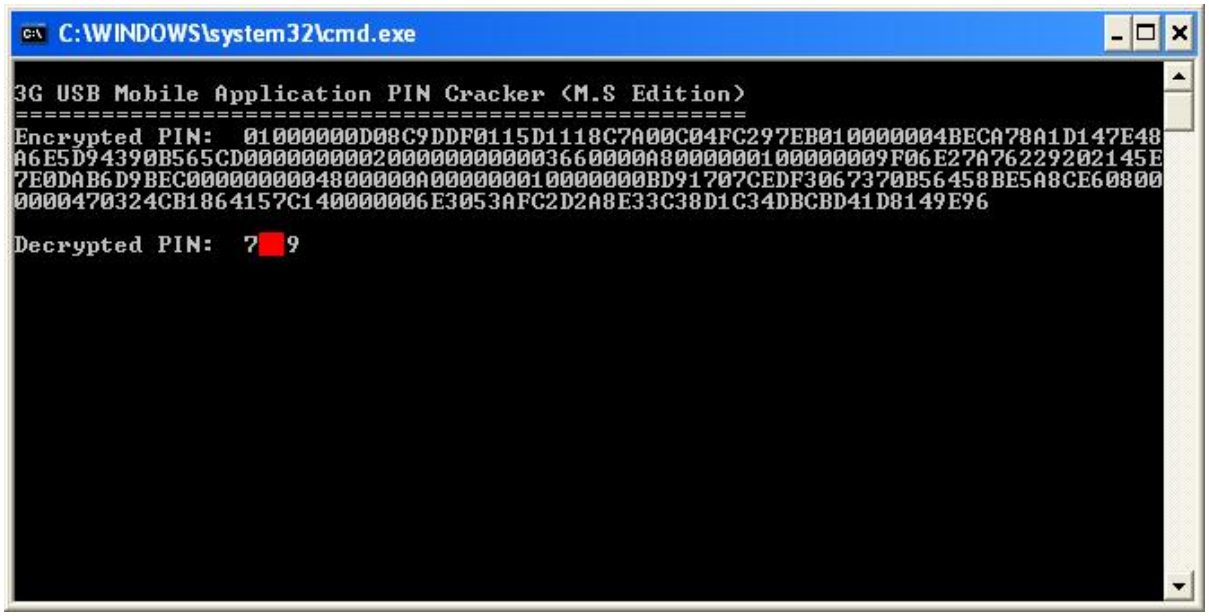
Bir trojan daha düşündüm, bir şekilde müşterinin bilgisayarında 3G USB modemin takılmasını beklesin ve daha sonrasında bu programı kullanarak usb modeme komutlar gönderebilsin. Peki ya neye yarayacaktı bu ? DDOS saldırılarının bir parçası olan zombie bilgisayarlar gibi sms flood yapmaya yarayan veya sms spam yapmaya yarayan zombie bilgisayarlar art niyetli insanların yeni hedefi olabilirdi. Peki trojanın bu komutları gönderebilmek için neye ihtiyacı vardı ? Tabiiki öncelikle doğru PIN’e çünkü mobil uygulama ilk açıldığında şayet save pin opsiyonu işaretlenmemişse kullanıcıdan PIN’i girmesi isteniyor ancak save pin opsiyonu işaretlenmiş ise arka plandan PIN şifrelenmiş xml dosyasından alınarak decrypt ediliyor ve modeme gönderiliyor.

Bu durumda save pin opsiyonu işaretlenmiş olan bir 3G USB modemin bilgisayara bağlı olması ve sadece flash disk niyetine kullanılması bile trojanın PIN'e ihtiyaç duyulan tüm işlemleri gerçekleştirebilmesine olanak sağlayabilir. Tabii bunun için öncelikle diskte şifreli olarak saklanan PIN'i kırması gerekiyor.

Buradan yola çıkarak PIN'in disk üzerinde nerede tutulduğunu aramaya koyuldum ve biraz araştırdıktan sonra X/UserData/XProfile.XML dosyası içerisinde yer aldığını gördüm. (Not: X, mobil uygulama adına göre değişmektedir.)

< pincode >
1;0;0;0;208;140;157;223;1;21;209;17;140;122;0;192;79;194;151;235;1;0;0;0;75;236;167;138;29;20;126;72;166;229;217;67;144;181;101;205;0;0;0;0;2;0;0;0;0;0;3;102;0;0;168;0;0;0;16;0;0;0;159;6;226;122;118;34;146;2;20;94;126;13;171;109;155;236;0;0;0;0;4;128;0;0;160;0;0;0;16;0;0;0;189;145;112;124;237;243;6;115;112;181;100;88;190;90;140;230;8;0;0;0;71;3;36;203;24;100;21;124;20;0;0;0;110;48;83;175;194;210;168;227;60;56;209;195;77;188;189;65;216;20;158;150;
< /pincode >

Görüldüğü üzere PIN, xml dosyasında şifreli olarak tutuluyordu. Sıra kullanılan şifrelemenin ne kadar başarılı olduğunu anlamaya gelmişti. Bunun için 3G mobil uygulamasını incelemeye başladım ve kısa bir süre içerisinde C# programlama dili ile yazılmış olduğunu gördüm. Konu C# olunca kaynak koduna ulaşmak ne kadar zor olabilirdi :) Classları 1 saat inceledikten sonra sonunda PIN'in Data Protection API ile şifrelendiğini anlamam ve python ile şifre çözücü programı hazırlamam yaklaşık 1 saat sürdü. Bu sayede Save PIN opsiyonunun PIN'inin güvenliğine önem verenler için kullanılmadan önce bir daha düşünülmesi gerektiğini söyleyebilecek noktaya geldim.



Mobil uygulama ile 3G usb modem arasındaki haberleşmeyi ise usb port monitör programı ile izlemeye başladığımda PIN'in doğrulama esnasında açık halde modeme gittiğini gördüm.

110 0.00039726 X.e IRP_MJ_WRITE QCUSB_COM9_2 SUCCESS Length 15:
AT+CPIN="7**9"
111 0.00001117 X.e IOCTL_SERIAL_GET_WAIT_MASK QCUSB_COM9_2 SUCCESS

Normalde Kobil mIdentity gibi USB akıllı kart okuyuculardaki doğrulamalarda, şifreler bu şekilde açık mı gidiyor bilmiyorum, pekte sanmıyorum ancak eğer açık gitmiyor ve teknik olarak mümkün ise ise mobil uygulamalar ve 3G USB modemler arasındaki iletişiminde şifreli olması güvenliği arttırabilir.

Sonuç olarak 3G USB mobil uygulamalardaki save pin opsiyonunun internet tarayıcılarındaki remember me opsiyonunda olduğu gibi riskli olduğunu, bunun dışında 1 Ocak tarihinden itibaren internet bankacılığında kullanılacak olan tek kullanımlık şifrenin 3G USB modem ile kullanılması durumunda trojanların hedefi olabileceğini ve son olarak 3G mobil uygulama ile 3G USB modem arasındaki haberleşmede PIN'in açık olarak transfer edildiğini (iyileştirmeye açık olabilir) sizlerle paylaşmak istedim. GSM operatörlerinde çalışan arkadaşlar dilerlerse konu ile ilgili yorum yaparak varsa eksik ve hatalı kısımları düzelterek beni ve herkesi aydınlatabilirler…